REMARKS

Claim Status

Applicants thank the Examiners, Ms. Trang T. Daon and Mr. Zia Syed, for the courtesies extended to applicants' representative during the telephone interview conducted on November 10, 2009, and for their assistance in furthering prosecution on the merits of the instant application. During the telephone interview, the subject matter of independent claims 1 and 12 was discussed. No agreement with respect to patentability of the claims was reached. The following remarks take into account the content of the telephone interview.

Claims 1, 3-10, 12 and 13 are now pending, with claims 1 and 12 being in independent form. Independent claims 1 and 12 have been amended. Support for the amendments may be found, for example, at pg. 8, lines 27-31 and pg. 8, line 36 to pg. 9, line 3 of the specification as originally filed. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

Overview of the Office Action

Claims 1, 3-10 and 12-13 stand rejected under 35 U.S.C. §103(a) as unpatentable over "Clustering Intrusion Detection Alarms to Support Root Cause Analysis", IBM Research, Zurich Research Laboratory, ACM Transactions on Information System Security, Vol. 6, No. 4, pgs. 443-474, November 2003 ("*Julisch*") in view of U.S. Patent No. 6,445,774 ("*Kidder*").

Applicants have carefully considered the Examiner's rejections, and the comments provided in support thereof. For the following reasons, applicants assert that all claims now pending in the present application are patentable over the cited art.

Patentability of the Independent Claims Under 35 U.S.C. §102(a)

Independent claim 1 has been amended to clarify the salient aspects of the claimed invention. Amended independent claim 1 now recites, *inter alia*, "completing the description of each of said alerts with sets of generalized valued attributes induced by the taxonomic structures based on the valued attributes of said alerts to form complete alerts". Independent claim 12 has been correspondingly amended. Support for this amendment may be found, for example, at pg. 8, lines 27-31 and pg. 8, line 36 to pg. 9, line 3 of the specification as originally filed. No new matter has been added.

The Examiner (at pg. 4 of the Office Action) acknowledges that *Julisch* does not disclose "consulting the complete alerts by at least one of successively interrogating and browsing said complete alerts so that the alert management system responds to a request by supplying pertinent valued attributes enabling a subset of complete alerts to be distinguished in a set of complete alerts satisfying the request to enable said request to be refined, said request being a logic formula of at least one of said valued attributes" as recited in independent claims 1 and 12, and cites *Kidder* for this feature.

Applicants respectfully disagree that the combination of *Julisch* and *Kidder* either teaches or suggests applicants' claimed invention as recited in now-amended independent claims 1 and 12.

Julisch discloses an intrusion detection system (IDS) which lists detected alarms within Alarm Logs. *Julisch* teaches that an algorithm is executed to organize the detected alarms into clusters, where all alarms belonging to the same cluster are characterized based on shared common attributes. In the *Julisch* system, a summary of each cluster is created to facilitate the

interpretation of each cluster by a single generalized alarm, where the generalization is based on a taxonomic structure.

Tables I and II on pgs. 452 and 464 of *Julisch* are examples of tables listing clusters of detected alarms, where each cluster is reported by a single generalized alarm. For example, *Julisch* (pg. 464) discloses Table II that includes generalized alarms of an alarm cluster. *Julisch* (pg. 465) provides a description of the contents of this table. More particularly, *Julisch* (pg. 464) depicts a table that includes generalized alarms of the alarm cluster. *Julisch* (pg. 465) explains the meaning of several examples of generalized alarms, e.g., WWW ITS *View Source Attack,* FTP SYST *Command Attempt*, which are contained in Table II shown at pg. 464.

However, *Julisch* absolutely fails to teach or suggest that the description of each alert is completed with sets of generalized valued attributes as required by now-amended independent claims 1 and 12. What *Julisch* does teach is that each alarm cluster is reported by a single generalized alarm (see, e.g., pg. 445, lines 19-20). *Julisch* does not teach that each alarm of a cluster has a description that is completed with a set of generalized valued attributes, as expressly required by now-amended independent claims 1 and 12.

The Examiner (at pg. 3-4 of the Office Action) asserts that:

> Julisch discloses ... completing the description of each of said alerts with sets of values induced by the taxonomic structures based on the valued attributes of said alerts to form complete alerts (Julisch: page 449, paragraphs 2-4), 'generalized alarm'); storing said completed alerts in a logic file system to enable said complete alerts to be consulted (Julisch: page 450, section 5.1 and 463-465, 'alarm log'); ***wherein each complete alert is saved in the logic file as a file with a completed description of each complete alert expressed using a propositional logic*** (Julisch: pages 449 and 460-463). (Emphasis Supplied)

Applicants disagree.

Julisch fails to disclose, teach or suggest the saving of complete alerts in a logic file system (LFS), where each complete alert is saved as a file with a completed description of each alert expressed using propositional logic. There is nothing whatsoever in *Julisch* describing or suggesting this expressly-recited subject matter of independent claims 1 and 12. Indeed, the Examiner has failed to provide any further explanation or reference to substantiate or support her assertion that the use of an LFS is taught in section 4, pg. 450 of *Julisch* (i.e., "*Alarm-clustering problems*").

Moreover, the text at pg. 449 of *Julisch* merely provides a definition of "an alarm", i.e., an Alarm Log and a generalized alarm. Neither the description provided at pg. 449, nor at any other page of *Julisch*, has anything to do with the storing of complete alarms within the meaning and scope of applicants' claimed invention. There is no teaching or suggestion in *Julisch* of the use of a logic file system (LFS) to store complete alarms.

Pages 460-463 of *Julisch* provide an explanation of how to best define appropriate generalization hierarchies for all possible alarm attributes, depending on the type of attributes at hand. More particularly, sections 6.1.1 to 6.1.3 of *Julisch* describe cases in which the alarms are expressed in terms of numerical values, time attributes and string attributes, respectively. The only storage which is contemplated or disclosed in *Julisch* is within the framework of storing context information for the purpose of facilitating the interpretation of detected alarms (see, e.g., pg. 460; "*String Attributes*"). There is no teaching or suggestion whatsoever in *Julisch* of an LFS or the storing of complete alarms. Section 6.2 of *Julisch* merely describes an example of the Alarm Log which, as explained above, only includes detected (i.e., non generalized) alarms. There is no storing operation in the manner expressly recited and claimed in independent claims 1 and 12.

Julisch thus fails to teach or suggest "storing said complete alerts in a logic file system to enable said complete alerts to be consulted", and that "each complete alert is saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic", as recited in independent claim 1 and correspondingly recited in independent claim 12.

Kidder likewise fails to teach or suggest saving or consulting "*complete alarms*" within the meaning and scope of applicants' claimed invention, i.e., alerts having a description that is completed with generalized valued attributes induced by a taxonomic structure. That is, *Kidder* fails to teach or suggest "completing the description of each of said alerts with sets of generalized valued attributes induced by the taxonomic structures based on the valued attributes of said alerts to form complete alerts", as recited in now-amended independent claim 1 and correspondingly recited in now-amended independent claim 12.

Kidder relates to "methods and systems for automating the dissemination and processing of alarm reports received from a telecommunications network", where each alarm report corresponds to an alarm detected in the telecommunication network (see Abstract, lines 1-6). *Kidder* (col. 8, lines 6-11; Fig. 5) explains that once a network monitor 404 has received alarm reports from the handling PM 401, the network monitor may "select one or more of these alarm reports to create an event using a 'create event' function". According to *Kidder*, "an event is a grouping of alarm reports to facilitate their processing" (Emphasis Supplied) (see col. 8, lines 6-13). *Kidder* (col. 6, lines 48-53; Fig. 2) explains that the network monitors 204 determine "the set of events that best represents the alarm reports" to facilitate processing of the alarm reports.

The Examiner's proffered analysis posits that these event reports of *Kidder* correspond to the complete alerts of independent claims 1 and 12. Applicants disagree. The alarms included in

an event report of *Kidder* constitute "raw" alarms, which are alarms whose description has not been completed with sets of generalized valued attributes induced by a taxonomic structure, as now required by amended independent claims 1 and 12. The alarms within the same cluster of *Kidder* are merely detected alarms which the network considers are linked to a particular event.

In fact, there is no disclosure, teaching or suggestion whatsoever in *Kidder* regarding completing the description of alerts or the use of a taxonomic structure. The network monitors 204 of *Kidder* merely create clusters of alarms by manually selecting "raw" detected alarms, each of which has a particular relationship to a specific event. Moreover, the selection of *Kidder* is performed manually, and selectively on an *ad hoc* basis (see, e.g., col. 2, lines 41-44 and lines 62-66). In any event, a taxonomic structure is not used to create these event reports. As with *Julisch, Kidder* fails to teach or suggest saving complete alerts as expressly required by independent claims 1 and 12.

Still further, *Kidder* fails to teach or suggest that alerts (complete or incomplete) are saved in a logic file system (LFS) as expressly recited in now-amended independent claims 1 and 12. *Kidder* also fails to teach or suggest complete alerts that can be consulted in response to a request, where the request is a logic formula of at least one valued attribute, as additionally recited in independent claims 1 and 12.

Kidder discloses that the network monitor (404) merely consults an event database (415). There is no teaching or suggestion of precisely how the events are organized by the network monitor or how these events can be consulted by the network monitor. Indeed, *Kidder* provides no indication whatsoever of the need or desire to save complete alarms in the event database (415).

Kidder (col. 12, lines 37-64) explains that the automated workstation system "adds to an alarm report a site identifier that identifies the location of the network component which generated the alarm". After adding the alarm report to the site identifier, the network monitors (404) can then select a specific site identifier to retrieve the associated detected alarms and insert these detected alarms into an event report. There is no teaching or suggestion in this section of *Kidder* of the expressly-recited subject matter of now-amended independent claims 1 and 12.

The combination of *Julisch* and *Kidder* thus fails to achieve the expressly recited subject matter of independent claims 1 and 12. *Julisch*, on the one hand, fails to teach or suggest saving or consulting complete alerts within a LES while *Kidder*, on the other hand, teaches saving clusters of "raw" alarms within a simple database, which differs substantially from the express recitations of independent claims 1 and 12. Accordingly, even assuming, *arguendo*, that the skilled person were to have a reason to combine the teachings of *Kidder* with those of *Julisch* in an effort to achieve the expressly-recited subject matter of independent claims 1 and 12, there would be no reason or motivation for the skilled person to further modify the system achieved by the combination of *Julisch* and *Kidder* so that complete alerts would be saved and consultable within an LFS.

The claimed invention advantageously eliminates the need to cluster alerts prior to saving these alerts in the LFS. In fact, it is the description of each alert that is completed and it is each completed alert that is saved in the LES, such that a user can customize his logic requests to consult any desired cluster of completed alerts within the LES. Put differently, a user can dynamically refine a search of completed descriptions within the LFS to locate alerts. The combination of *Julisch* and *Kidder* fails to teach or suggest applicants' claimed invention that encompasses such advantageous features and functionality.

For example, *Kidder* requires that each alarm cluster be statically defined by a network monitor and then saved within a database (415). *Kidder* provides a system in which it is not possible to refine a search of alarms within the database (415) using requests expressed as a logic formula, let alone that the alarms of *Kidder* are not provided with a completed description of the alarm. The *Kidder* system simply allows the network monitors to retrieve predefined clusters of alarms. *Kidder* thus teaches away from the expressly-recited subject matter of independent claims 1 and 12. In addition, as explained above, the network monitors in *Kidder* manually select the alarms on an *ad hoc* basis to build a cluster of alarms. *Kidder* teaches away from the use of a taxonomic structure which defines generalized relationships between valued attributes of the alarms.

Julisch and/or *Kidder*, whether considered individually or in combination, therefore fail to teach or suggest the express recitations of independent claims 1 and 12.

Reconsideration and withdrawal of the rejection of claims 1 and 12 as unpatentable over the combination of *Julisch* and *Kidder* under 35 U.S.C. §103 are accordingly deemed to be in order, and early notice to that effect is solicited.

Dependent Claims

In view of the patentability of independent claims 1 and 12 for the reasons presented above, each of dependent claims 2-10 and 13 is respectfully deemed to be patentable therewith over the prior art. Moreover, each of these claims includes features which serve to still further distinguish the claimed invention over the applied art.

Conclusion

Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are once more solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By /Lance J. Lieberman/
Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: November 25, 2009